ABSTRACT

A general-purpose central processing unit (CPU) is configured with a new mechanism that facilitates an authenticated boot sequence. The boot sequence provides the building blocks for client-side rights management when the system is online, and provides for continued protection of persistent data even when the system goes offline or is rebooted. The CPU is manufactured with a cryptographic key pair, a manufacturer certificate testifying that the manufacture built the CPU according to a known specification, and an optional immutable symmetric key K_S. The operating system includes a unique block of code, referred to as the "boot block". An OS identity can be established from the boot block by extracting the identity from a digitally signed the boot block or by computing a hash digest of the boot block. During booting, the CPU executes a single opcode, followed by the boot block, as an atomic operation to set the identity of the operating system into the software identity register. Execution of the opcode and the boot block is atomic, such that the software identity register is set to either the OS identity (i.e., boot block digest or OS public key) if the combined operation is successful, or zero if something subverts operation. Assuming success, the CPU appends the OS identity to its boot log. Following this authenticated boot sequence, the subscriber unit can establish a chain of trust to prove its hardware and software to a content provider. The subscriber unit stores content from the content provider in encrypted form using a storage key that is generated as a function of OS-specific and CPU-specific data, so that it can be decrypted only on the same processor and by the specified OS.